(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 759 675 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.02.1997 Bulletin 1997/09

(51) Int Cl.[6]: **H04N 7/167**

(21) Application number: **96202140.8**

(22) Date of filing: **29.07.1996**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU NL PT SE

(30) Priority: **10.08.1995 NL 1000964**

(71) Applicant: **Koninklijke PTT Nederland N.V.**
9726 AE Groningen (NL)

(72) Inventors:
- **Hekstra, Andries Pieter**
  2252 KM Voorschoten (NL)
- **van Tilburg, Johan**
  2719 KK Zoetermeer (NL)

(74) Representative: **van Bommel, Jan Peter et al**
Koninklijke PTT Nederland N.V.,
P.O. Box 95321
2509 CH Den Haag (NL)

(54) Method for providing access to information by way of enciphering/deciphering messages including transmitting and receiving devices

(57) Known methods for, by way of enciphering/deciphering messages, providing access to information, per authorised user transmit an enciphered message which, since only an authorised user disposes of a deciphering method, may be deciphered by him only. By transmitting the same message to all users, which message has been enciphered per user by way of an enciphering method associated with said user if said user has not been authorised, and has not been enciphered if said user has been authorised, with a user not disposing of the deciphering method associated with him and disposing of the deciphering methods associated with other users, all users receive this same message, while only the authorised users may decipher the enciphered message and may gain access to the information by way of the message deciphered by them, and the unauthorised users cannot gain access to the information by way of the message still enciphered for them, and the method is given an efficient nature.

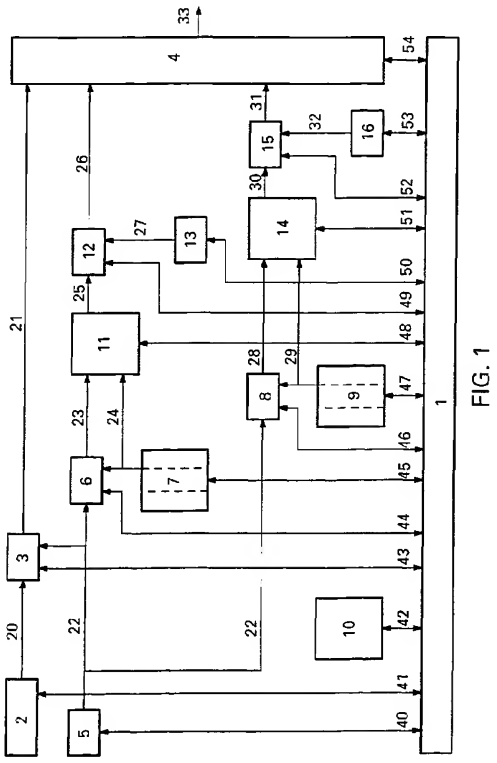

FIG. 1

EP 0 759 675 A1

Description

A. BACKGROUND OF THE INVENTION

The invention relates to a method for, by way of enciphering/deciphering messages, providing authorised users with access to information, and not providing unauthorised users with access to information.

Such a method is of general knowledge and proceeds as follows. If a user is authorised, he disposes of a deciphering method for deciphering an enciphered message while, if said user is not authorised, he does not dispose of the deciphering method. As a result, an authorised user may decipher the message, which deciphered message provides him with access to certain information, while an unauthorised user cannot decipher the message, as a result of which he does not gain access to the information. Said information might, e.g., be recorded in the message, or is, e.g., transmitted to a user only after said user has returned the deciphered message, or is, e.g., transmitted to the user in enciphered state, with said user being capable of deciphering the enciphered information only on the basis of the deciphered message.

Such a method has the drawback, inter alia, that per authorised user a message has to be transmitted, which in the event of many users connected to a few nodes results in many messages to be serially transmitted, which give the known method an inefficient nature, with every user additionally seeing all (enciphered) messages passing.

B. SUMMARY OF THE INVENTION

The object of the invention is, inter alia, to provide a method of the kind referred to in the preamble, with which providing access to the information proceeds in a more efficient way.

For this purpose, the method according to the invention is characterised in that the method comprises the steps of

- per unauthorised user enciphering a message by way of an enciphering method associated with said unauthorised user,
- per authorised user not enciphering the message by way of an enciphering method associated with said authorised user,
- transmitting the message to the users,
- receiving the message by the users, with every user not disposing of a deciphering method associated with said user for deciphering a message enciphered by way of the enciphering method associated with said user, and disposing of deciphering methods associated with other users for deciphering a message enciphered by way of enciphering methods associated with said other users,
- in the event of at least one unauthorised user, per authorised user deciphering the message enciphered by way of the enciphering methods associated with unauthorised users and gaining access, by said authorised user, to the information by way of the deciphered message,
- in the event of no unauthorised user, per authorised user gaining access, by said authorised user, to the information by way of the non-enciphered message, and
- not gaining access, by unauthorised users, to the information by way of the enciphered message.

By transmitting the same message to the users in question, which message has been enciphered per user by way of an enciphering method associated with said user if said user is not authorised, and has not been enciphered by way of the enciphering method associated with said user if said user has been authorised, the users in question receive this same message while, since every user does not dispose of a deciphering method associated with said user for deciphering a message enciphered by way of an enciphering method associated with said user and does dispose of deciphering methods associated with other users for deciphering a message enciphered by way of enciphering methods associated with said other users, only the authorised users can decipher the enciphered message and can gain access to the information by way of the message deciphered by them, and the unauthorised users cannot gain access to the information by way of the message still enciphered for them, with, in the event of no unauthorised users, of course all authorised users being capable of gaining access to the information by way of the non-enciphered message. As a result, only one and the same message needs to be transmitted to the users in question, and the method according to the invention has a very efficient nature.

The invention is based, inter alia, on the insight that it is much more efficient to transmit one and the same enciphered message to all users (with only authorised users being capable of gaining access, by way of the deciphered message, to the information) than per next user to transmit a next, enciphered message.

Thus, the problem of the known method being inefficient is solved by transmitting the same message to the users in question, which message has been enciphered per user by way of an enciphering method associated with said user if said user has not been authorised, and has not been enciphered if said user has been authorised, with in this case every user not being permitted to dispose of a deciphering method associated with said user for deciphering a message enciphered by way of an enciphering method associated with said user, and has to dispose of deciphering methods associated with other users for deciphering a message enciphered by way of enciphering methods associated with said other users.

A first embodiment of the method according to the

invention is characterised in that the information is enciphered by way of the non-enciphered message and can be deciphered only by way of the non-enciphered or deciphered message.

By enciphering the information by way of the non-enciphered message, with the information enciphered in this manner only being capable of being deciphered by way of the non-enciphered or deciphered message, only authorised users gain access to said information.

A second embodiment of the method according to the invention is characterised in that the message is enciphered prior to transmission by way of a further enciphering method, with the enciphered message being deciphered after receipt by way of a further deciphering method.

By enciphering the message prior to transmission by way of a further enciphering method, and after receipt deciphering it by way of a further deciphering method, the message is always transmitted in enciphered state, even if all users in question have been authorised, which benefits the security.

A third embodiment of the method according to the invention is characterised in that a total number of users is distributed over a number of user groups, with a message being transmitted per user group.

By distributing a total number of users over a number of user groups, with one message being transmitted per user group, every user admittedly sees just as many messages passing as there are user groups, but said user only needs to decipher the message associated with his user group and said user only needs to dispose of the number of deciphering methods associated with all other users belonging to the same user group.

The invention further relates to a transmitter device for transmitting data messages to users for providing access to information for authorised users and not providing access to information for unauthorised users, which transmitter device is provided with

- an enciphering device for per user being capable of enciphering a data message by way of an enciphering method associated with said user, and
- an adding device for adding to the data message a user-identification signal.

Such a transmitter device is of general knowledge and operates as follows. Per user and by way of the enciphering device, the data message is enciphered by way of the enciphering method associated with said user, and the user-identification signal is added, by way of the adding device, to the data message, and the enciphered data message is transmitted to said user. If the user has been authorised, he disposes of a deciphering method for deciphering the enciphered data message while, if said user has not been authorised, he does not dispose of the deciphering method. As a result, an authorised user may decipher the data message, which deciphered data message provides him with access to certain information, while an unauthorised user cannot decipher the data message, as a result of which he does not gain access to the information.

Such a transmitter device has the drawback, inter alia, that per authorised user one data message has to be transmitted, which in the event of many users being connected to a few nodes results in many data messages to be transmitted serially which give the known whole an inefficient nature, with additionally every user seeing all (enciphered) messages passing.

The object of the invention, inter alia, is to provide a transmitter device of the kind referred to above, with which providing access to the information proceeds in a more efficient way.

For this purpose, the transmitter device according to the invention is characterised in that the transmitter device is provided with

- a generator device for per user generating an authentication signal which has a first value in the event of an unauthorised user and which has a second value in the event of an authorised user,

with the enciphering device being provided with a control input for per user receiving the authentication signal for, in response to an authentication signal having a first value, enciphering the data message by way of an enciphering method associated with said unauthorised user and for, in response to an authentication signal having a second value, not enciphering the data message by way of an enciphering method associated with said authorised user.

By generating, by way of the generator device, an authentication signal per user which has a first value in the event of an unauthorised user and which has a second value in the event of an authorised user, with the enciphering device being provided with the control input for per user receiving the authentication signal for, in response to an authentication signal having a first value, enciphering the data message by way of an enciphering method associated with said unauthorised user and for, in response to an authentication signal having a second value, not enciphering the data message by way of an enciphering method associated with said authorised user, the same data message may be transmitted to the users in question, which data message has been enciphered per user by way of an enciphering method associated with said user if said user has not been authorised, and has not been enciphered if said user has been authorised, and the users in question receive this same data message. If every user does not dispose of a deciphering method associated with said user for deciphering a data message enciphered by way of an enciphering method associated with said user, and does dispose of deciphering methods associated with other users for deciphering a data message enciphered by way of enciphering methods associated with said other us-

ers, only the authorised users may decipher the enciphered data message and gain access to the information by way of the data message deciphered by them, and the unauthorised users cannot gain access to the information by way of the data message still enciphered for them, with, in the event of no unauthorised users, of course all authorised users being capable of gaining access to the information by way of the non-enciphered data message. As a result, only one and the same data message needs to be transmitted to the users in question, and the whole according to the invention has a very efficient nature.

A first embodiment of the transmitter device according to the invention is characterised in that the transmitter device is provided with

- enciphering means for, by way of the data message, enciphering the information to be transmitted to the users.

By enciphering the information by way of enciphering means, with the information thus enciphered being capable of being deciphered only by way of the non-enciphered or deciphered data message, only authorised users gain access to said information.

A second embodiment of the transmitter device according to the invention is characterised in that the transmitter device is provided with

- a further enciphering device coupled to the enciphering device for enciphering the message by way of a further enciphering method.

By enciphering the data message prior to transmission by way of the further enciphering device, with, after receipt, it having to be deciphered by way of a further deciphering method, the data message is always transmitted in enciphered state, even if all users in question have been authorised, which benefits the security.

A third embodiment of the transmitter device according to the invention is characterised in that a total number of users is distributed over a number of user groups, with the transmitter device transmitting a data message per user group.

By distributing a total number of users over a number of user groups, with the transmitter device transmitting one data message per user group, every user admittedly sees just as many data messages passing as there are user groups, but said user only needs to decipher the data message associated with his user group and said user only needs to dispose of the number of deciphering methods associated with all other users belonging to the same user group.

The invention still further relates to a receiver device for receiving a data message for providing access to information for an authorised user and not providing access to information for an unauthorised user, which receiver device is provided with

- a detection device for detecting a user-identification signal added to the data message.

Such a receiver device is of general knowledge and operates as follows. Per user and by way of a transmitter device, the data message is deciphered by way of a deciphering method associated with said user, and a user-identification signal is added to the data message by way of the transmitter device, and the enciphered and amended data message is transmitted to said user. By way of the detection device, the user-identification signal added to the data message is detected, on the basis whereof it is established whether or not said data message is intended for said receiver device. If the user has been authorised, his receiver device disposes of a deciphering method for deciphering the enciphered data message while, if said user has not been authorised, his receiver device does not dispose of the deciphering method. As a result, an authorised user may decipher the data message, which deciphered data message provides him with access to certain information, while an unauthorised user cannot decipher the data message, as a result of which he does not gain access to the information.

Such a receiver device has the drawback, inter alia, that per authorised user one data message has to be transmitted, which in the event of many users being connected to a few nodes results in many data messages to be transmitted serially, which give the known whole an inefficient nature, with additionally every user seeing all (enciphered) messages passing.

A still further object of the invention, inter alia, is to provide a receiver device of the kind referred to above, with which providing access to the information proceeds in a more efficient way.

For this purpose, the receiver device according to the invention is characterised in that the receiver device is provided with

- a further detection device coupled to the detection device for, from the user-identification signal, detecting at least one authentication signal associated with another user which has a first value in the event of an unauthorised other user and which has a second value in the event of an authorised other user,
- a deciphering device coupled to the further detection device for, in response to at least one authentication signal associated with another user having a first value, deciphering the data message by way of a deciphering method associated with said unauthorised other user, and, in response to at least one authentication signal associated with another user having a second value, not deciphering the data message by way of a deciphering method associated with said authorised other user.

By detecting, by way of the further detection device from the user-identification signal, at least one authen-

tication signal associated with another user which has a first value in the event of an unauthorised other user and which has a second value in the event of an authorised other user, and deciphering, by way of the deciphering device in response to at least one authentication signal associated with another user having a first value, the data message by way of a deciphering method associated with said unauthorised other user, and in response to at least one authentication signal associated with another user having a second value, not deciphering the data message by way of a deciphering method associated with said authorised other user, the same data message may be transmitted to the users in question, which data message has been enciphered per user by way of an enciphering method associated with said user if said user has not been authorised, and has not been enciphered if said user has been authorised, and the users in question receive this same data message. Only the authorised users may decipher the enciphered data message and gain access to the information by way of the data message deciphered by them, while, in the event of no unauthorised users, of course all authorised users may gain access to the information by way of the non-enciphered data message. As a result, only one and the same data message needs to be transmitted to the users in question and the whole according to the invention has a very efficient nature.

A first embodiment of the receiver device according to the invention is characterised in that the receiver device is provided with

- deciphering means for, by way of the deciphered or non-enciphered data message, deciphering the information to be received.

By enciphering the information by way of the transmitter device, with the information enciphered in this manner only being capable of being deciphered by way of the deciphering means, only authorised users gain access to said information.

A second embodiment of the receiver device according to the invention is characterised in that the receiver device is provided with

- a further deciphering device coupled to the deciphering device for deciphering the message by way of a further deciphering method.

If the data message is enciphered prior to transmission by way of the transmitter device, with, after receipt, it then having to be deciphered by way of the further deciphering device, the data message may always be transmitted in enciphered state, even if all users in question have been authorised, which benefits the security.

A third embodiment of the receiver device according to the invention is characterised in that a total number of users is distributed over a number of user groups, with the receiver device being provided with

- detection means for detecting a data message associated with a certain user group.

By distributing a total number of users over a number of user groups, with a transmitter device transmitting one data message per user group, every user admittedly sees just as many data messages passing as there are user groups, but said user needs to detect, by way of the detection means, and to decipher only the data message associated with his user group, and said user needs to dispose of only the number of deciphering methods associated with all other users belonging to the same user group.

EP 0 641 103 discloses a method and a device for distributing keys in a selectively transmitting system. In this case, every receiver disposes not of his own key but of the keys of all other receivers. The transmitter by way of a combination key transmits encrypted information, which combination key is obtained by modulo-2 addition of those keys which belong to all unauthorised receivers. Since unauthorised receivers do not dispose of their own keys, they cannot, knowing which receivers are unauthorised, imitate the combination key, while authorised receivers, knowing which receivers are unauthorised, may imitate the combination key, as a result of which the encrypted information can be decrypted only by the authorised receivers with the help of the combination key. A drawback here is, inter alia, that adding/removing an authorisation immediately leads to a modified combination key, with which the information is encrypted, as a result of which said adding/removing of an authorisation may take place either only at a very limited number of moments without great technical problems arising, or occurs at arbitrary moments, involving great technical problems. Neither the method according to the invention, nor the devices according to the invention, are disclosed in this patent.

C. REFERENCES

- EP 0 641 103
- "Tracing Trators", by Benny Chor and Amos Fiat and Moni Naor, Advances in Cryptology, Crypto '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994
- "Broadcast Encryption", by Amos Fiat and Moni Naor, Advances in Cryptology, Crypto '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-25, 1993
- "Contemporary Cryptology", The Science of Information Integrity, edited by Gustavus J. Simmons, IEEE press, 1992
- "Cryptography: a new dimension in computer data

security", A guide for the Design and Implementation of Secure Systems, by Carl H. Meyer and Stephen M. Matyas, A Wiley-Interscience Publication, John Wiley & Sons, 1982

All references are considered to be incorporated in the this patent application.

D. EXEMPLARY EMBODIMENT

The invention will be explained in greater detail by reference to an exemplary embodiment shown in the figures. Here,

FIG. 1 shows a transmitter device according to the invention for application in the method according to the invention, and
FIG. 2 shows a receiver device according to the invention for application in the method according to the invention.

The transmitter device according to the invention shown in FIG. 1 comprises an information source 2 which is coupled, by way of a control connection 41, to a processor 1 and of which an output is coupled, by way of a connection 20, to a first input of enciphering means 3. Furthermore, the transmitter device shown in FIG. 1 comprises a message memory 5 which is coupled, by way of a control connection 40, to processor 1 and of which an output is coupled, by way of a connection 22, to a second input of enciphering means 3 and to a first input of a first enciphering device 6 and to a first input of a second enciphering device 8. A processor memory 10 is coupled, by way of a control connection 42, to processor 1; enciphering means 3 are coupled, by way of a control connection 43, to processor 1; first enciphering device 6 is coupled, by way of a control connection 44, to processor 1; and second enciphering device 8 is coupled, by way of a control connection 46, to processor 1. An output of enciphering means 3 is coupled, by way of a connection 21, to a first input of multiplexer 4. A second input of first enciphering device 6 is connected, by way of a connection 24, to an output of a first table memory 7 which is coupled, by way of a control connection 45, to processor 1. A second input of second enciphering device 8 is connected, by way of a connection 29, to an output of a second table memory 9 which is coupled, by way of a control connection 47, to processor 1. An output of first enciphering device 6 is coupled, by way of a connection 23, to a first input of a first adding device 11 which is coupled, by way of a control connection 48, to processor 1 and of which a second input is connected, by way of connection 24, to the output of first table memory 7. An output of second enciphering device 8 is coupled, by way of a connection 28, to a first input of a second adding device 14 which is coupled, by way of a control connection 51, to processor 1 and of which a second input is connected, by way of connection 29, to the output of second table memory 9. An output of first adding device 11 is coupled, by way of a connection 25, to a first input of a third enciphering device 12 which is coupled, by way of a control connection 49, to processor 1 and of which a second input is connected, by way of a connection 27, to an output of a first code memory 13 which is coupled, by way of a control connection 50, to processor 1. An output of second adding device 14 is coupled, by way of a connection 30, to a first input of a fourth enciphering device 15 which is coupled, by way of a control connection 52, to processor 1 and of which a second input is connected, by way of a connection 32, to an output of a second code memory 16 which is coupled, by way of a control connection 53, to processor 1. An output of third enciphering device 12 is coupled, by way of a connection 26, to a second input of multiplexer 4, and an output of fourth enciphering device 15 is coupled, by way of a connection 31, to a third input of multiplexer 4 of which an output is connected to a connection 33 and which is coupled, by way of a control connection 54, to processor 1.

The operation of the transmitter device shown in FIG. 1 is as follows. A Pay-TV video signal to be transmitted is stored in information source 2. Prior to the transmission thereof, the being authorised or not of users belonging to a first user group has to be recorded in first table memory 7, and the being authorised or not of users belonging to a second user group has to be recorded in second table memory 9. For this purpose, both table memories 7 and 9 each dispose of three columns - a first column for per row storing a user identity, a second column for per row storing the being authorised or not of the associated user, and a third column for per row storing an enciphering method coupled to the associated user. Generally, the data stored in the first and the third column will already be present, or be stored for a longer period of time, while the data required in the second column will have to be established per Pay-TV video signal to be transmitted, and loaded into both table memories 7 and 9. This is then done by way of the control connections 45 and 47, and by way of processor 1. Per Pay-TV video signal to be transmitted, there is further established a message which, by way of control connection 40 and by way of processor 1, is loaded into message memory 5.

Message memory 5 receives, by way of control connection 40, a command signal originating from processor 1 and generates, in response thereto, the stored message which is fed, by way of connection 22, to enciphering means 3, and to first enciphering device 6 and to second enciphering device 8. Enciphering means 3 further receive, by way of connection 20, the Pay-TV video signal originating from information source 2, which is transmitted by information source 2 in response to a command signal to be received by way of control connection 41 and originating from processor 1, and encipher said Pay-TV video signal on the basis of the message under control of control signals to be received by

way of control connection 43 and originating from processor 1, whereafter the enciphered video signal is fed to multiplexer 4 by way of connection 21.

First table memory 7 receives, by way of control connection 45, a command signal originating from processor 1 and consecutively generates, in response thereto, a first group identification and (part of) the data stored per row (or per user identification), with the first group identification and all user identifications and user authorisations stored in the first and second columns per row (or per user identification) being fed, by way of connection 24, to first adding device 11 while, of the enciphering methods stored in the third column, only the enciphering methods associated with the unauthorised users are fed, by way of connection 24, to first enciphering device 6. Under control of control signals to be received by way of control connection 44 and originating from processor 1, first enciphering device 6 enciphers the arrived message according to the enciphering methods associated with the unauthorised users, e.g., by consecutively applying said enciphering methods in a certain order to the message. Subsequently, first enciphering device 6 feeds the message thus enciphered in a first manner, under control of processor 1, to first adding device 11 by way of connection 23. First adding device 11 combines, in response to control signals originating from processor 1 and to be received by way of control connection 48, the message enciphered in a first manner with the first group identification and all user identifications and user authorisations stored in first table memory 7, and feeds the combined whole, under control of processor 1, to third enciphering device 12 by way of connection 25. First code memory 13 receives, by way of control connection 50, a command signal originating from processor 1 and generates, in response thereto, a first code which is fed, by way of connection 27, to third enciphering device 12. Under control of control signals to be received by way of control connection 49 and originating from processor 1, third enciphering device 12 enciphers the arrived combined whole on the basis of the first code. Subsequently, third enciphering device 12 feeds the whole thus enciphered by way of the first code, under control of processor 1, to multiplexer 4 by way of connection 26.

Second table memory 9 receives, by way of control connection 47, a command signal originating from processor 1 and consecutively generates, in response thereto, a second group identification and (part of) the data stored per row (or per user identification), with the second group identification and all user identifications and user authorisations stored in the first and second columns per row (or per user identification) being fed, by way of connection 29, to second adding device 14 while, of the enciphering methods stored in the third column, only the enciphering methods associated with the unauthorised users are fed, by way of connection 29, to second enciphering device 8. Under control of control signals to be received by way of control connection 46 and originating from processor 1, second enciphering device 8 enciphers the arrived message according to the enciphering methods associated with the unauthorised users, e.g., by consecutively applying said enciphering methods in a certain order to the message. Subsequently, second enciphering device 8 feeds the message thus enciphered in a second manner, under control of processor 1, to second adding device 14 by way of connection 28. Second adding device 14 combines, in response to control signals originating from processor 1 and to be received by way of control connection 51, the message enciphered in a second manner with the second group identification and all user identifications and user authorisations stored in second table memory 9, and feeds the combined whole, under control of processor 1, to fourth enciphering device 15 by way of connection 30. Second code memory 16 receives, by way of control connection 53, a command signal originating from processor 1 and generates, in response thereto, a second code which is fed, by way of connection 32, to fourth enciphering device 15. Under control of control signals to be received by way of control connection 52 and originating from processor 1, fourth enciphering device 15 enciphers the arrived combined whole on the basis of the second code. Subsequently, fourth enciphering device 15 feeds the whole thus enciphered by way of the second code, under control of processor 1, to multiplexer 4 by way of connection 31.

Under control of control signals to be received by way of control connection 54 and originating from processor 1, multiplexer 4 combines the enciphered video signal with the whole enciphered by way of the first code and the whole enciphered by way of the second code, whereafter the result is transmitted, by way of connection 33, to at least the users belonging to the first and the second user groups.

The receiver device shown in FIG. 2 according to the invention comprises a demultiplexer 101, of which an input is connected to connection 33 and which is coupled, by way of a control connection 140, to a processor 100. A first output of demultiplexer 101 is coupled, by way of a connection 120, to a first input of deciphering means 102 which are coupled, by way of a control connection 147, to processor 100. An output of deciphering means 102 is connected to a connection 121 for coupling to an information processor such as, e.g., a television set, and a second input of deciphering means 102 is connected to an output of a first deciphering device 107 by way of a connection 127. A first input of first deciphering device 107 is coupled to a first output of a splitting device 105 by way of a connection 125, and a second input of first deciphering device 107 is connected, by way of a connection 128, to an output of a third table memory 108 which is coupled, by way of a control connection 146, to processor 100. By way of a control connection 145, first deciphering device 107 is coupled to processor 100. A second output of splitting device 105 is coupled, by way of a connection 126, to an input of a

data memory 106 which is coupled, by way of a control connection 144, to processor 100. An input of splitting device 105 is connected, by way of a connection 124, to an output of a second deciphering device 103, while splitting device 105 is coupled, by way of a control connection 143, to processor 100. A first input of second deciphering device 103 is coupled, by way of a connection 122, to a second output of demultiplexer 101 and a second input is connected, by way of a connection 123, to an output of a third code memory 104 which is coupled, by way of a control connection 142, to processor 100. By way of a control connection 141, second enciphering device 103 is coupled to processor 100.

The operation of the receiver device shown in FIG. 2 is as follows, it being assumed that said receiver device is associated with an authorised user belonging to the first user group (in the transmitter device, the message then has therefore not been enciphered by way of the enciphering method associated with said authorised user, but has possibly been enciphered by way of the enciphering methods associated with other, unauthorised users). Under control of control signals to be received by way of control connection 140 and originating from processor 100, demultiplexer 101 separates the enciphered video signal from the whole enciphered by way of the first code and the whole enciphered by way of the second code, whereafter the enciphered video signal is fed, by way of connection 120, to deciphering means 102 and the whole enciphered by way of the first code is fed, by way of connection 122, to second deciphering device 103. Third code memory 104 receives, by way of control connection 142, a command signal originating from processor 100 and generates, in response thereto, a third code which is fed, by way of connection 123, to second deciphering device 103. Under control of control signals to be received by way of control connection 141 and originating from processor 100, second deciphering device 103 deciphers the whole enciphered by way of the first code on the basis of the third code. In general, the first code and the third code will be equal in this case. Subsequently, second deciphering device 103 feeds the whole thus deciphered by way of the third code, under control of processor 100, to splitting device 105 by way of connection 124.

Splitting device 105 splits, in response to control signals originating from processor 100 and to be received by way of control connection 143, the whole deciphered by way of the third code into, on the one hand, the message enciphered in a first manner and, on the other hand, the first group identification and all user identifications and user authorisations, and under control of processor 100 feeds the message enciphered in a first manner to first deciphering device 107 by way of connection 125 and feeds, under control of processor 100, the first group identification and all user identifications and user authorisations to data memory 106 by way of connection 126. Processor 100 detects, by way of control connection 144, that the first group identification has been stored in data memory 106 (e.g., by comparison to a third group identification stored in table memory 108 and to be fed, by way of control connection 146, to processor 100, which third group identification then has to match the first group identification), as a result of which it has been established that said data is indeed intended for said receiver device.

Third table memory 108 disposes of three columns - a first column for per row storing a user identity, a second column for per row storing the being authorised or not of the associated user, and a third column for per row storing an enciphering method coupled to the associated user. In general, the data stored in the first and the third column will already be present, or be stored for a longer period of time, while the data required in the second column will have to be established per Pay-TV video signal to be transmitted, and be loaded into table memory 108. This is done under control of processor 100 by feeding the user identifications and user authorisations stored in data memory 106, by way of control connection 144 and by way of processor 100 and by way of control connection 146, to third table memory 108.

Third table memory 108 receives, by way of control connection 146, a command signal originating from processor 100 and consecutively generates, in response thereto, (part of) the data per row (or per user identification) stored in the third column while, of the deciphering methods stored in the third column, only the deciphering methods associated with the unauthorised users are fed, by way of connection 128, to first deciphering device 107. Under control of control signals to be received by way of control connection 145 and originating from processor 100, first deciphering device 107 deciphers the enciphered message according to the deciphering methods associated with the unauthorised users, e.g., by consecutively applying said deciphering methods in a certain order (inverted with respect to the transmitter device) to the message. Subsequently, first deciphering device 107 feeds the thus deciphered message, under control of processor 100, to deciphering means 102 by way of connection 127.

Deciphering means 102 receive, by way of control connection 147, control signals originating from processor 100 and decipher, in response thereto, the enciphered video signal on the basis of the deciphered message to be received by way of connection 127, whereafter the original Pay-TV video signal may be viewed by way of connection 121 and by way of, e.g., the television set.

For the operation of the receiver device shown in FIG. 2 in so far as the whole enciphered in the transmitter device by way of the second code is concerned, which is therefore intended for another (second) user group, there are at least three options. In the first place, demultiplexer 101 might already make a selection, e.g., by ignoring a certain time interval, so that the whole enciphered by way of the second code does not pass demultiplexer 101. In the second place, the whole enci-

phered by way of the second code might, e.g., since it is separated in time from the whole enciphered by way of the first code, pass demultiplexer 101 and might, some time after the whole enciphered by way of the first code has been offered, be offered to second deciphering device 103 while, since the second code differs from the third code stored in the third code memory, this time there is effected no correct deciphering here, as a result of which splitting device 105 and/or data memory 106 will have to deal with gibberish.

In the third place, the whole enciphered by way of the second code might, e.g., since it is separated in time from the whole enciphered by way of the first code, pass demultiplexer 101 and might, some time after the whole enciphered by way of the first code has been offered, be offered to second deciphering device 103 while, since the second code this time does not differ from the third code stored in the third code memory, there is effected a correct deciphering here. In response to control signals originating from processor 100 and to be received by way of control connection 143, splitting device 105 splits the whole deciphered by way of the third code into, on the one hand, the message enciphered in a second manner and, on the other hand, the second group identification and all user identifications and user authorisations, and splitting device 105 feeds, under control of processor 100, the message enciphered in a second manner to first deciphering device 107 by way of connection 125, and splitting device 105 feeds, under control of processor 100, the second group identification and all user identifications and user authorisations to data memory 106 by way of connection 126. Processor 100 detects, by way of control connection 144, that another (the second) group identification is stored in data memory 106 (e.g., by comparison to a third group identification stored in table memory 108 and to be fed, by way of control connection 146, to processor 100, which third group identification then has to match the first group identification), as a result of which it is established that said data is not intended for said receiver device. Independently from said detection, of course, the message enciphered in a second manner will generally not be capable of being deciphered in a correct manner by way of first deciphering device 107.

The operation of the receiver device shown in FIG. 2, if it is assumed that said receiver device is associated with a user belonging to the first user group but this time unauthorised (in the transmitter device, the message then is therefore enciphered by way of the enciphering method associated with said unauthorised user and possibly still further enciphered by way of enciphering methods associated with other, unauthorised users and therefore not enciphered by way of the enciphering methods associated with the remaining authorised users of said user group), is in accordance with the above, with the exception of the following.

Third table memory 108 receives, by way of control connection 146, a command signal originating from processor 100 and consecutively generates, in response thereto and for feeding, by way of connection 128, to first deciphering device 107, the deciphering methods stored in the third column which are associated with the unauthorised users, with the exception of the deciphering method associated with said unauthorised user who manages the receiver device. Not generating said one deciphering method either is, e.g., the result of said deciphering method not being present in said table memory 108, or all this is the result of said one deciphering method admittedly being present but on the contrary being deactivated in said table memory 108. This time, first deciphering device 107 does therefore not succeed in deciphering the enciphered message according to the deciphering methods associated with the unauthorised users, since one of said deciphering methods is not available. As a result, a still enciphered message is fed to deciphering means 102, with which the enciphered video signal cannot be deciphered.

If the Pay-TV video signal is an analogue signal, enciphering means 3 and deciphering means 102 are film coders and film decoders known to those skilled in the art. Multiplexer 4 and demultiplexer 101 then are, e.g., so-called television chips with which there may be combined analogue video signals and digital teletext signals (and therefore also enciphered messages and user identifications etc.). If the Pay-TV video signal is a digital signal, enciphering means 3 and deciphering means 102 are, e.g., so-called encryption chips and decryption chips which each convert, e.g., a 64-bit input word as a function of, e.g., a 64-bit key word into a 64-bit output word. The enciphering devices 6, 8, 12 and 15 and the deciphering devices 103 and 107 might also be realised with encryption chips and decryption chips. In this case, the messages and the enciphering methods and the deciphering methods therefore comprise so-called keys.

The concept of "information" should be interpreted as having the broadest possible significance. Not only might it therefore concern a Pay-TV video signal, but an option also is to transmit, e.g., by way of a cable network, aviation information to the homes of aviation personnel with, e.g., a first part of the aviation personnel being fully authorised, while a second and a third part of the aviation personnel is each authorised only with respect to a different part of the aviation information. Apart from this, the information might be transmitted, e.g., by way of the electric mains, to homes of users with in this case, e.g., the boilers and/or sun screens of only authorised users being capable of being driven. Also, the concept of "by way of enciphering/deciphering messages, providing access to information" should be interpreted as having the broadest possible significance, since the information source and the message source might coincide as well as be geographically separated, while the information in certain cases might even be completely recorded in the messages (the deciphered or non-enciphered message then matches, in whole or in part, the information).

If a user buys or hires a receiver device, said receiv-

er device will generally already be provided with a user identification (e.g., stored in data memory 106 and/or in table memory 108) and a standard deciphering method and/or standard key (generally stored in code memory 104). The first message to be transmitted to said receiver device then has to be enciphered in the transmitter device by way of a standard enciphering method and/or standard key (generally stored in code memory 13 and/or 16), and is deciphered in the receiver device, whereafter the receiver device is loaded with the data present in the deciphered message such as, e.g., a new code (which is generally stored in code memory 104) and a group identification and user identifications of users belonging to the same group (which are stored, e.g., in data memory 106 and/or in table memory 108) and associated deciphering methods and/or keys (which are stored, e.g., in table memory 108). Also, extending and/or amending and/or modifying data already stored in the receiver device will generally be effected by way of one or more messages. In this case, messages may be provided with an indication, which indication indicates that said message is mainly intended for deciphering device 107 and/or deciphering means 102, or indicates that the message is mainly intended for adjusting data, and which indication has to be detected by way of splitting device 105 and/or data memory 106 and/or processor 100.

Claims

1. Method for, by way of enciphering/deciphering messages, providing access to information for authorised users and not providing access to information for unauthorised users, characterised in that the method comprises the steps of

   - per unauthorised user, enciphering a message by way of an enciphering method associated with said unauthorised user,
   - per authorised user, not enciphering the message by way of an enciphering method associated with said authorised user,
   - transmitting the message to the users,
   - receiving the message by the users, with each user not disposing of a deciphering method associated with said user for deciphering a message enciphered by way of the enciphering method associated with said user and, on the other hand, disposing of deciphering methods associated with other users for deciphering a message enciphered by way of enciphering methods associated with said other users,
   - in the event of at least one unauthorised user, per authorised user deciphering the message enciphered by way of the enciphering methods associated with unauthorised users and gaining access, by said authorised user, to the information by way of the deciphered message,
   - in the event of no unauthorised user, per authorised user gaining access, by said authorised user, to the information by way of the non-enciphered message, and
   - gaining no access, by unauthorised users, to the information by way of the enciphered message.

2. Method according to claim 1, characterised in that the information is enciphered by way of the non-enciphered message and may be deciphered only by way of the non-enciphered or deciphered message.

3. Method according to claim 1 or 2, characterised in that the message is enciphered prior to transmission by way of a further enciphering method, the enciphered message after receipt being deciphered by way of a further deciphering method.

4. Method according to claim 1, 2 or 3, characterised in that a total number of users is distributed over a number of user groups, a message being transmitted per user group.

5. Transmitter device for transmitting data messages to users for providing access to information for authorised users and not providing access to information for unauthorised users, which transmitter device is provided with

   - an enciphering device for being capable of per user enciphering a data message by way of an enciphering method associated with said user, and
   - an adding device for adding to the data message a user-identification signal,

   characterised in that the transmitter device is provided with

   - a generation device for per user generating an authentication signal which has a first value in the event of an unauthorised user and which has a second value in the event of an authorised user,

   the enciphering device being provided with a control input for per user receiving the authentication signal for enciphering, in response to an authentication signal having a first value, the data message by way of an enciphering method associated with said unauthorised user and not enciphering, in response to an authentication signal having a second value, the data message by way of an enciphering method associated with said authorised user.

6. Transmitter device according to claim 5, character-

ised in that the transmitter device is provided with

- enciphering means for enciphering, by way of the data message, the information to be transmitted to the users.

7. Transmitter device according to claim 5 or 6, characterised in that the transmitter device is provided with

- a further enciphering device coupled to the enciphering device for enciphering the message by way of a further enciphering method.

8. Transmitter device according to claim 5, 6 or 7, characterised in that a total number of users is distributed over a number of user groups, the transmitter device transmitting a data message per user group.

9. Receiver device for receiving data messages for providing access to information for an authorised user and not providing access to information for an unauthorised user, which receiver device is provided with

- a detection device for detecting a user-identification signal added to the data message,

characterised in that the receiver device is provided with

- a further detection device coupled to the detection device for detecting, from the user-identification signal, at least one authentication signal associated with another user which has a first value in the event of an unauthorised other user and which has a second value in the event of an authorised other user,
- a deciphering device coupled to the further detection device for deciphering, in response to at least one authentication signal associated with another user having a first value, the data message by way of a deciphering method associated with said unauthorised other user and not deciphering, in response to at least one authentication signal associated with another user having a second value, the data message by way of a deciphering method associated with said authorised other user.

10. Receiver device according to claim 9, characterised in that the receiver device is provided with

- deciphering means for deciphering, by way of the deciphered or non-enciphered data message, the information to be received.

11. Receiver device according to claim 9 or 10, characterised in that the receiver device is provided with

- a further deciphering device coupled to the deciphering device for deciphering the message by way of a further deciphering method.

12. Receiver device according to claim 9, 10 or 11, characterised in that a total number of users is distributed over a number of user groups, the receiver device being provided with

- detection means for detecting a data message associated with a certain user group.

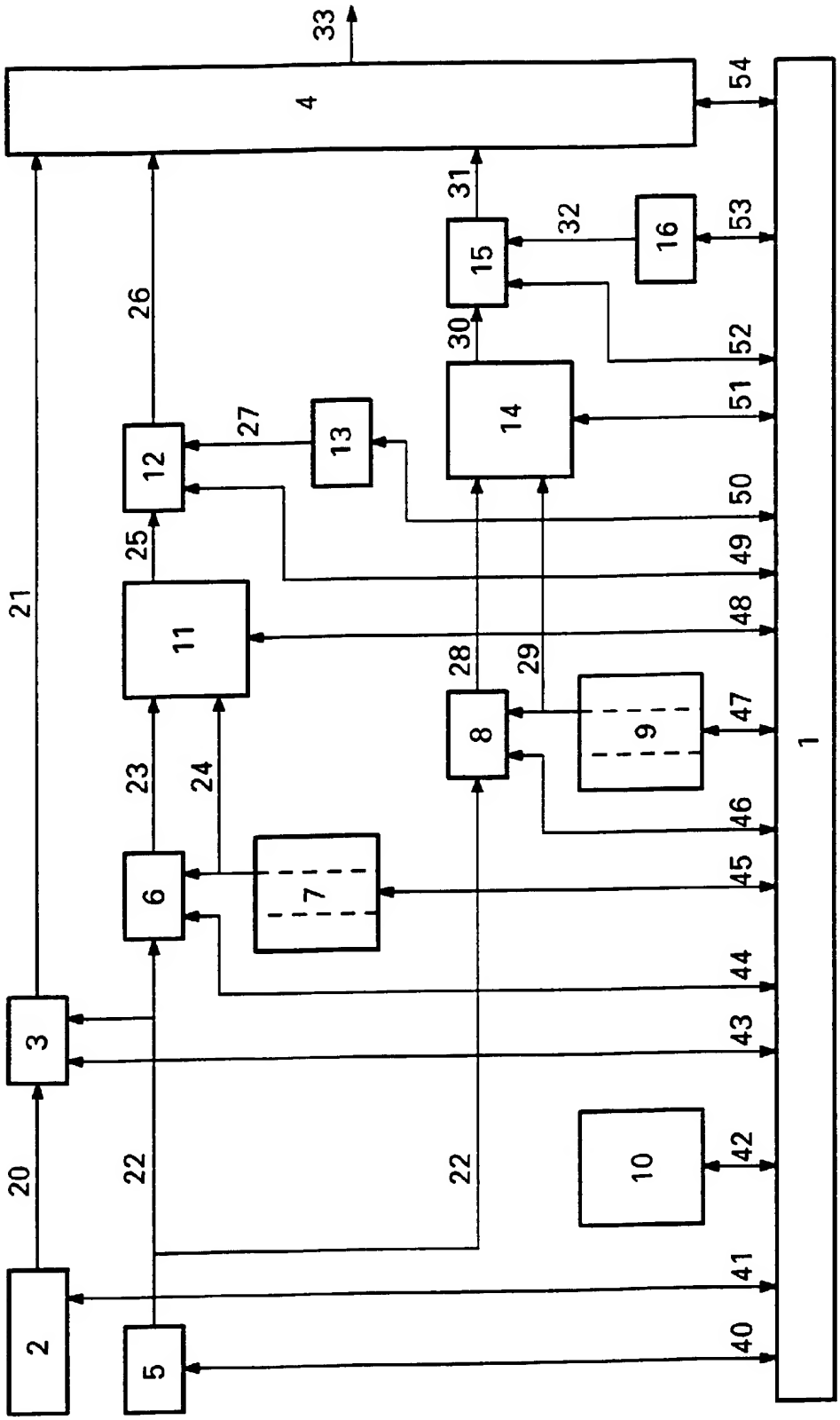
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
20
21
22
23
24
25
26
27
28
29
30
31
32
33
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54

FIG. 1

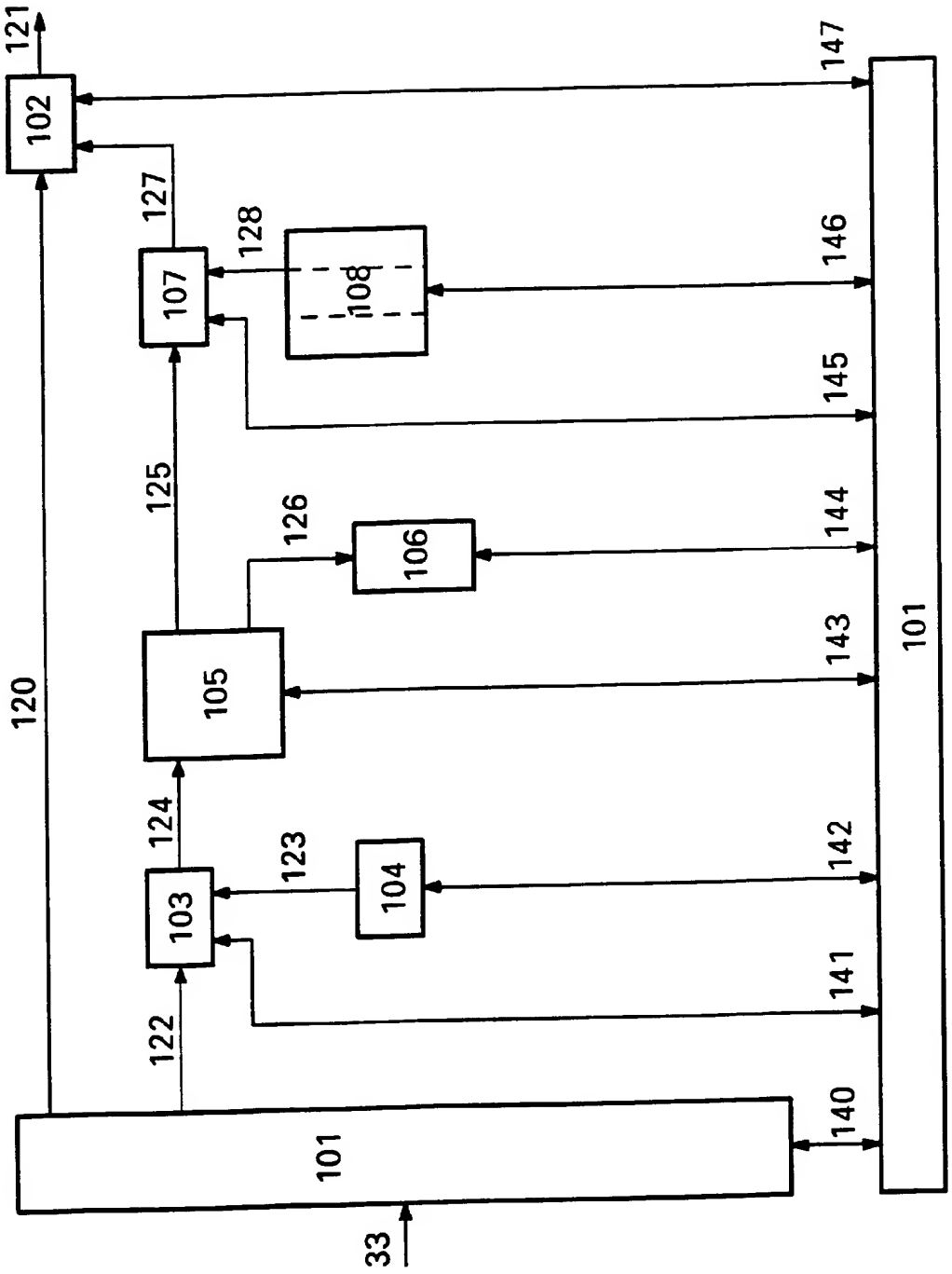
121
102
147
127
128
107
108
146
145
125
126
106
144
105
143
101
120
124
123
104
142
103
141
122
101
140
33

FIG. 2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 96 20 2140

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP-A-0 343 805 (GEN INSTRUMENT CORP) 29 November 1989 * abstract * * page 4, column 6, line 35 - page 12, column 22, line 48 * * figures 1-8 *	1-12	H04N7/167
X	EP-A-0 256 596 (PHILIPS ELECTRONICS UK LTD ;PHILIPS NV (NL)) 24 February 1988 * abstract * * page 2, column 1, line 20 - column 2, line 4 * * page 4, column 5, line 39 - page 5, column 8, line 55 * * figures 1-3 *	1-3,5-7, 9-11	
A	EP-A-0 438 145 (STEGMAIER HANS PETER) 24 July 1991 * page 3, column 3, line 3 - line 21 * * page 3, column 4, line 50 - page 4, column 6, line 17 * * page 6, column 9, line 21 - column 10, line 41 * * figures 1,4,5 *	1-12	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04N
A	IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 38, no. 3, 1 August 1992, pages 188-194, XP000311835 ANGEBAUD D ET AL: "CONDITIONAL ACCESS MECHANISMS FOR ALL-DIGITAL BROADCAST SIGNALS"		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	6 September 1996	Van der Zaal, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)